Risks of File-Sharing Technology

Cyber Security Tip ST05-007

File-sharing technology is a popular way for users to exchange, or "share," files. However, using this technology makes you susceptible to risks such as infection, attack, or exposure of personal information.

What is file sharing?

File sharing involves using technology that allows internet users to share files that are housed on their individual computers. Peer-to-peer (P2P) applications, such as those used to share music files, are some of the most common forms of file-sharing technology. However, P2P applications introduce security risks that may put your information or your computer in jeopardy.

What risks does file-sharing technology introduce?

- Installation of malicious code - When you use P2P applications, it is difficult, if not impossible, to verify that the source of the files is trustworthy. These applications are often used by attackers to transmit malicious code. Attackers may incorporate spyware, viruses, Trojan horses, or worms into the files. When you download the files, your computer becomes infected (see Recognizing and Avoiding Spyware and Recovering from Viruses, Worms, and Trojan Horses for more information).

- Exposure of sensitive or personal information - By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft (see Protecting Your Privacy and Avoiding Social Engineering and Phishing Attacks for more information).

- Susceptibility to attack - Some P2P applications may ask you to open certain ports on your firewall to transmit the files. However, opening some of these ports may give attackers access to your computer or enable them to attack your computer by taking advantage of any vulnerabilities that may exist in the P2P application. There are some P2P applications that can modify and penetrate firewalls themselves, without your knowledge.

- Denial of service - Downloading files causes a significant amount of traffic over the network. This activity may reduce the availability of certain programs on your computer or may limit your access to the internet (see Understanding Denial-of-Service Attacks for more information).

- Prosecution - Files shared through P2P applications may include pirated software, copyrighted material, or pornography. If you download these, even unknowingly, you may be faced with fines or other legal action. If your computer is on a company network and exposes customer information, both you and your company may be liable.

How can you minimize these risks?

The best way to eliminate these risks is to avoid using P2P applications. However, if you choose to use this technology, you can follow some good security practices to minimize your risk:

- use and maintain anti-virus software - Anti-virus software recognizes and protects your computer against most known viruses. However, attackers are continually writing new viruses, so it is important to keep your anti-virus software current (see Understanding Anti-Virus Software for more information).

- install or enable a firewall - Firewalls may be able to prevent some types of infection by blocking malicious traffic before it can enter your computer (see Understanding Firewalls for more information). Some operating systems actually include a firewall, but you need to make sure it is enabled.

Both the National Cyber Security Alliance and US-CERT have identified this topic as one of the top tips for home users.

Authors: Mindi McDowell, Brent Wrisley, Will Dormann

Produced 2007 by US-CERT, a government organization.

This document can also be found at: http://www.us-cert.gov/cas/tips/ST04-003.html

For instructions on subscribing to or unsubscribing from this mailing list, visit http://www.us-cert.gov/cas/signup.html.